Artificial Intelligence (AI) for Safety-Critical Systems

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Promising technologies for ECS
22nd September 2022

Jon Perez
jmperez@ikerlan.es
(INSIDE SC)

VISIT…

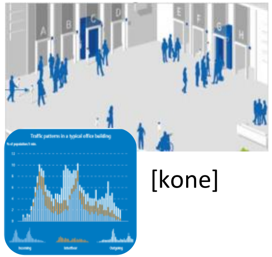
LANZAROTE Caliente.com

AGENDA

- Introduction
- Safety standards
- ML development (training)
- ML development (inference)
- Trustworthiness
- Conclusion

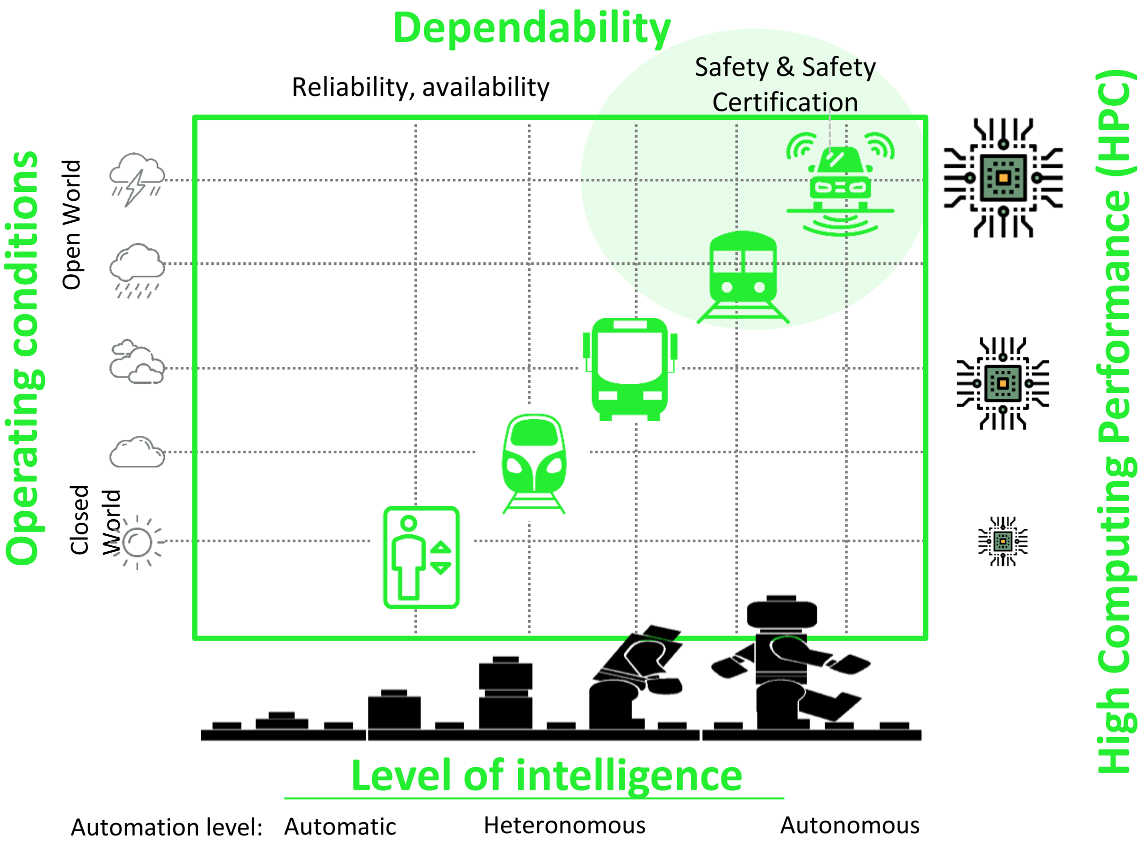
Example AI and dependable / Safety systems

[guard]



[kone]

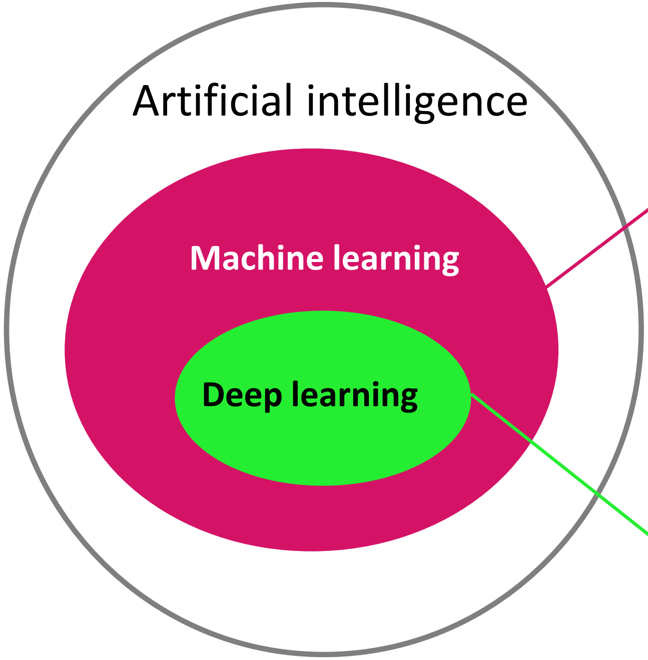
[Pe20b]



[ver]

[mov]

Machine learning



[Pe20b]

Linear regression.
Logistic regression.
Bayesian networks.
Decision tree.
Greedy algorithm.
Support Vector Machine (SVM).
Naive bayes.
Random forest.
Gradient boosting algorithm.
....

Neural Network (NN).
Deep learning.
Recurrent Neural Network (RNN).
Long Short Term Memory (LSTM).
.....

Artificial Intelligence [ISO 22989]:

"set of methods or automated entities that together build, optimize and apply a model so that the system can, for a given set of predefined tasks, compute predictions, recommendations, or decisions"

Machine Learning [Oxford]:

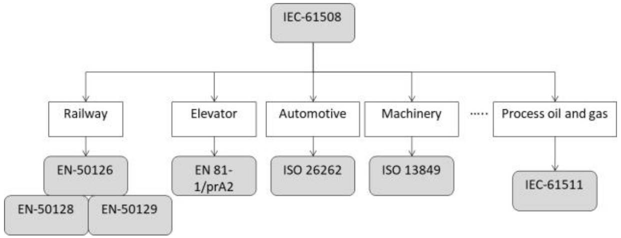
"the use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyze and draw inferences from patterns in data"

Scope


Updates
ML Development (Training)
ML Development (Training)
SAFETY STANDARDS
Trustworthiness

Safety standards

Functional Safety (Traditional)



Het./Autonomous Systems Artificial intelligence

Drafts:

- **ISO/PAS 21448**: Road vehicles — Safety of the intended functionality (**SOTIF**).
- **UL 4600** - Safety for the evaluation of autonomous products.
- **ISO/IEC AWI TR 5469**: artificial intelligence — functional safety and AI systems.
- **VDE-AR-E 2842-61-1**: Development and trustworthiness of autonomous/cognitive systems
- Etc.

Working Groups: EUROCA WG-114, SAE G-34, etc.

Scope

Updates

ML Development (Training)

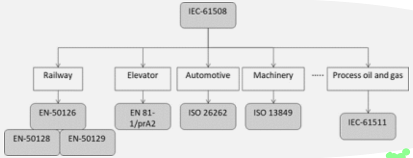
ML Development (Training)

SOTIF, UL 4600, IEC 5469

Artificial intelligence, autonomous systems and safety (draft) standards

Safety standards

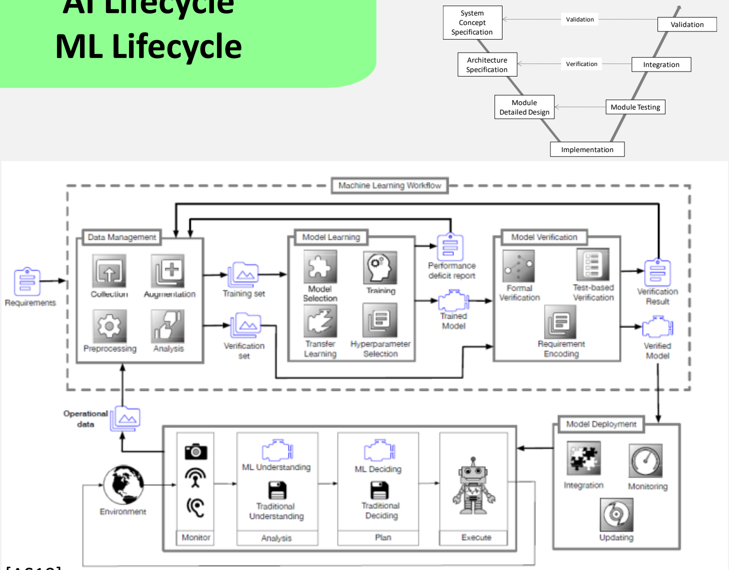
Functional safety standards: electronics / programmable electronics



Trustworthiness

Safety standards

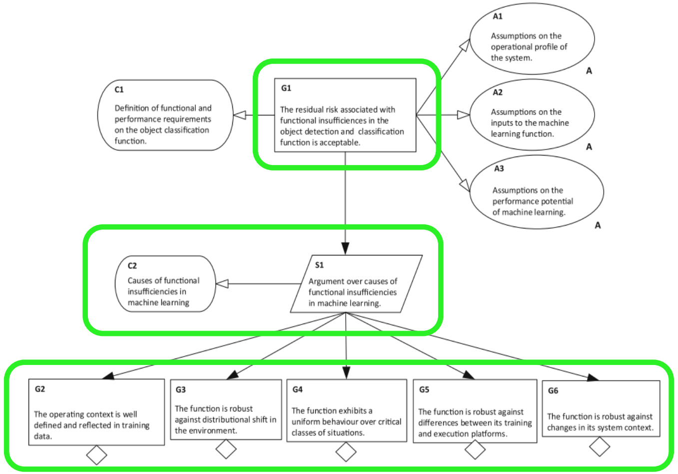
AI Lifecycle
ML Lifecycle



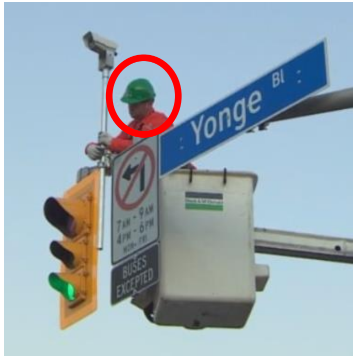
[AS19]

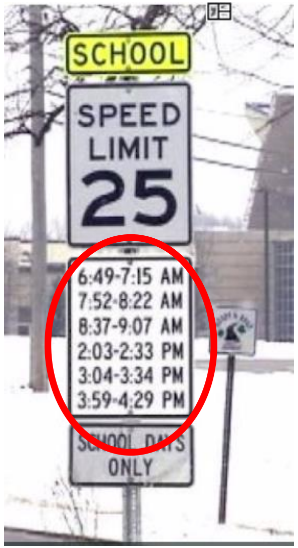
Fig. 1. The machine learning lifecycle

Example safety case
[Bu17] – GSN



Development (training)





[cbc, hre, Ka18]

Scope

Updates

ML Development (Training)

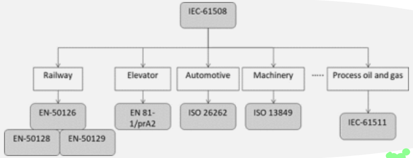
ML Development (Training)

SOTIF, UL 4600, IEC 5469

Artificial intelligence, autonomous systems and safety (draft) standards

Safety standards

Functional safety standards: electronics / programmable electronics



Trustworthiness

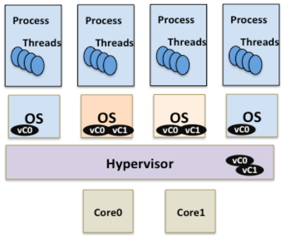
Deployment (inference)

Hardware device

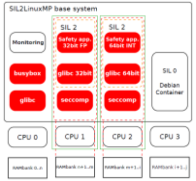
- Multi-core devices and MPSoCs [Pe20]
- GPUs [Ko19, Le18, Pe22]
- FPGAs [Ko19]
- Specialized devices, e.g., TPU
- Proprietary devices, e.g. Tesla FSD [Ta20]

Software

Hypervisor



Operating system



Domain specific runtime env.

Parallel Programming Runtimes

High-Performance Embedded Computing (HPEC) – Hardware and software.

- Safety compliance of ‘Parallel Programming runtime’ and ‘ML software libraries’ .
- Temporal Independence, guarantees and diagnosis [Pe20].
- Spatial independence [Pe20].
- Diagnosistic coverage (DC) [Pe20].
- Thermal dissipation, energy consumption [Ko19].

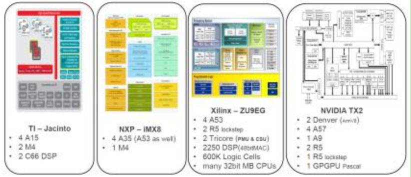
Deployment (inference)

Hardware device

- Multi-core devices and MPSoCs [Pe20]
- GPUs [Ko19, Le18, Pe22]
- FPGAs [Ko19]
- Specialized devices, e.g., TPU
- Proprietary devices, e.g. Tesla FSD [Ta20]

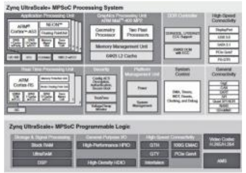
[Co17]

Generic purpose computing



[Co17] [nvidia]

Safety Std. Compliance and support



[xilinx]

Specialized computing solutions

[mbeye]

High-Performance Embedded Computing (HPEC) – Hardware and software.

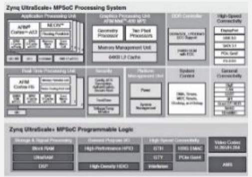
- Safety compliance of ‘Parallel Programming runtime’ and ‘ML software libraries’ .
- Temporal Independence, guarantees and diagnosis [Pe20].
- Spatial independence [Pe20].
- Diagnosistic coverage (DC) [Pe20].
- Thermal dissipation, energy consumption [Ko19].

Scope

Updates

ML Development (Training)

ML Development (Training)

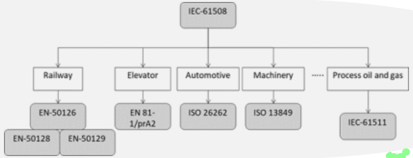


SOTIF, UL 4600, IEC 5469

Artificial intelligence, autonomous systems and safety (draft) standards

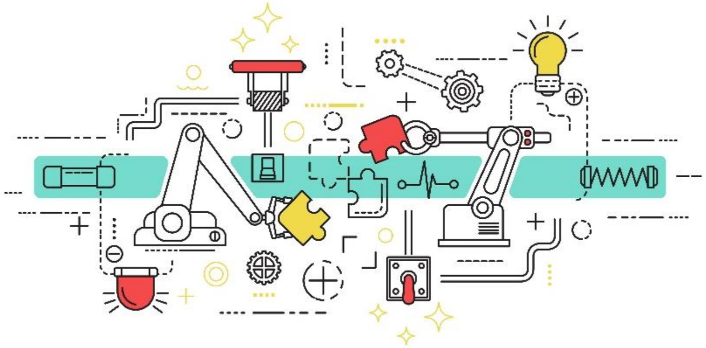
Safety standards

Functional safety standards: electronics / programmable electronics



Trustworthiness

Trustworthiness



Engineering

Ethics

Legal

Engineering Ethics

Machine Ethics

EUROPEAN COMMISSION

Brussels, 21.4.2021

COM(2021) 206 final

2021/0106(COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

CONCLUSION

There is a need to pave the way towards the development and certification of AI-based safety systems:

- Need for AI safety standard(s) definition and consolidation, complementary with functional safety standards.
- Many ML technical challenges: training data coverage (e.g., corner cases), understability, testability, verifiability, etc.
- Evolution of HPC challenges (HW / SW): integration of functions of different criticality in a HPC safe execution platform:
  - Safety compliance of ML libraries and parallel programming languages.
  - Temporal and spatial independence.
  - Thermal and energy requirements.
- Trustworthiness: Engineering, Ethics and Legal
- Safe and secure update of systems

References

- [AS19] R. Ashmore, R. Calinescu, and C. Paterson, "Assuring the Machine Learning Lifecycle: Desiderata, Methods, and Challenges," ArXiv, vol. abs/1905.04223, 2019.
- [AV04] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," in IEEE Transactions on Dependable and Secure Computing, January/March 2004, vol. 1, pp. 11-33
- [Bu17] S. Burton, L. Gauerhof, and C. Heinzemann, "Making the Case for Safety of Machine Learning in Highly Automated Driving," in Computer Safety, Reliability, and Security, Cham, S. Tonetta, E. Schoitsch, and F. Bitsch, Eds., 2017: Springer International Publishing, pp. 5-16.
- [Bo18] U. bodemhausen, "Deep learning and functional safety," in ESE Kongress, 2018
- [cbc] https://www.cbc.ca/news/canada/toronto/smart-traffic-signals-1.4417573
- [Co17] Giulio Corradi, Xilinx, Tools, Architectures and Trends on Industrial all Programmable Heterogeneous MPSoC, ECRTS (Keynote talk), 2017
- [guard] https://www.theguardian.com/world/2018/sep/23/potsdam-inside-the-worlds-first-autonomous-tram
- [HE18] J. Henriksson, M. Borg, and C. Englund, "Automotive Safety and Machine Learning: Initial Results from a Study on How to Adapt the ISO 26262 Safety Standard," in IEEE/ACM 1st International Workshop on Software Engineering for AI in Autonomous Systems (SEFAIAS), 28-28 May 2018, pp. 47-49.
- [IEC61508] IEC 61508-4: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations, IEC 61508, 2010.
- [Ka18] Karpathy, Andrej, “Building the Software 2.0 Stack”, 2018
- [KN02] J. C. Knight, "Safety critical systems: challenges and directions," in 24rd International Conference on Software Engineering (ICSE 2002), 2002, pp. 547-550.
- [Ko19] L. Kosmidis, J. Lachaize, J. Abella, O. Notebaert, F. J. Cazorla, and D. Steenari, "GPU4S: Embedded GPUs in Space," in 22nd Euromicro Conference on Digital System Design (DSD), 28-30 Aug. 2019, pp. 399-405, doi: 10.1109/DSD.2019.00064.
- [kone] https://guinea.kone.com/Images/brochure-kone-polaris_tcm170-18639.pdf
- [Le18] G. Lentaris et al., "High-Performance Embedded Computing in Space: Evaluation of Platforms for Vision-Based Navigation," Journal of Aerospace Information Systems, vol. 15, no. 4, pp. 178-192, 2018, doi: 10.2514/1.I010555.
- [MA19] R. Mariani, "Challenges in AI/ML for Safety Critical Systems (Key Note)," in 32nd IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2019: NVIDIA.
- [mbeye] https://www.mobileye.com/our-technology/evolution-eyeq-chip/
- [mov] Tenerife prueba un autobús eléctrico de Vectia. 2018; https://movilidadelectrica.com/tenerife-prueba-un-autobus-electrico-de-vectia/
- [nvidia] https://www.anandtech.com/show/15245/nvidia-details-drive-agx-orin-a-herculean-arm-automotive-soc-for-2022
- [Pe14] Perez, Jon; Alonso, Alejandro; Crespo, Alfons; “Tutorial: Developing Mixed-Criticality Systems with GNAT/ORK and Xtratum”, DATE Workshop, 2014
- [Pe20] J. Perez Cerrolaza et al., "Multi-core Devices for Safety-critical Systems: A Survey," ACM Comput. Surv., vol. 53, no. 4, July 2020, doi: https://doi.org/10.1145/3398665.
- [Pe20b] Perez, Jon; “Challenges of artificial intelligence and dependable systems - A focus on safety”, HIPEAC 2020
- [Pe22] J. Perez-Cerrolaza, J. Abella, L. Kosmidis, A. J. Calderon, F. J. Cazorla, and J. L. Flores, "GPU Devices for Safety-Critical Systems: A Survey," ACM Comput. Surv., 2022, doi: 10.1145/3549526.
- [Pl18] Andreas Platschek, Nicholas Mc Guire, Lukas Bulwahn; “Certifying Linux: Lessons Learned in Three Years of SIL2LinuxMP”, Embedded World, 2018
- [RA21] Nijat Rajabli et. Al., Software Verification and Validation of Safe Autonomous Cars: A Systematic Literature Review, IEEE Access, 2021
- [rhe] https://www.reporterherald.com/2019/10/31/dinosaur-big-brown-bear-help-children-cross-the-street-at-berthoud-elementary/
- [Ro17]. Royuela, A. Duran, M. A. Serrano, E. Quiñones, and X. Martorell. 2017. A Functional Safety OpenMP* for Critical Real-Time Embedded Systems. Springer, Book section 16.
- [Ta20] E. Talpes et al., "Compute Solution for Tesla's Full Self-Driving Computer," IEEE Micro, vol. 40, no. 2, pp. 25-35, 2020, doi: 10.1109/MM.2020.2975764.
- [ver] https://www.theverge.com/2018/5/9/17307156/google-waymo-driverless-cars-deep-learning-neural-net-interview
- [xilinx] https://www.xilinx.com/support/documentation/user_guides/ug1085-zynq-ultrascale-trm.pdf

THANK YOU

www.ikerlan.es

P.º J. M.ª. Arizmendiarrieta, 2 - 20500 Arrasate-Mondragón

T. +34 943 712 400 F. +34 943 796 944